**What is claimed is:**

1.     An apparatus for use in predicting exchanges of a specific quantity of communication traffic between network elements, said apparatus comprising:

a digital processor operable on a periodic basis to calculate a weighted traffic flow per usage for a given network element, said digital processor further including,

a comparison mechanism for comparing a value of said weighted traffic flow per usage with a remainder value of said specific quantity of communications traffic yet to be processed by said network element, wherein an indication is given by said network element if said remainder value is less than said weighted traffic flow.

2.     The apparatus of Claim 1, wherein said digital processor waits until beginning another time period to calculate another value of said weighted traffic flow per usage to be compared with an updated remainder value.

3.     The apparatus of Claim 1, wherein said specific quantity of communications traffic corresponds to a quantity value associated with a security association (SA) between said network elements.

4.     The apparatus of Claim 3, wherein said indication given from said network elements prompts renegotiation of another SA.

5.     The apparatus of Claim 3, wherein said SA is an Internet Protocol Security (IPSEC) SA.

6.     The apparatus of Claim 1, wherein said apparatus is used in connection with a communications traffic monitoring application to identify randomly occurring traffic patterns.

7.     The apparatus of Claim 1, wherein said apparatus is used in connection with a communications network management application to monitor usage of network components.

1  8.  The apparatus of Claim 1, wherein said weighted traffic flow per usage
2  corresponds to the average use of network element per period multiplied by the average
3  communications traffic quantity per use.

1  9.  A method of predicting exchanges of a specific quantity of communication
2  traffic between network elements, said method comprising:
3  calculating on a periodic basis a weighted traffic flow per usage for a given
4  network element;
5  comparing a value of said weighted traffic flow per usage with a remainder value
6  of said specific quantity of communications traffic yet to be processed by said network
7  element; and
8  giving an indication from said network element if said remainder value is less
9  than said weighted traffic flow.

1  10.  The method of Claim 9, further including waiting until beginning another
2  time period to calculate another value of said weighted traffic flow per usage to be
3  compared with an updated remainder value..

1  11.  The method of Claim 9, wherein said specific quantity of communications
2  traffic corresponds to a quantity value associated with a security association (SA)
3  between said network elements.

1  12.  The method of Claim 11, wherein said indication given from said network
2  elements prompts renegotiation of another SA.

1  13.  The method of Claim 11, wherein said SA is an Internet Protocol Security
2  (IPSEC) SA.

1  14.  The method of Claim 1, wherein said method is used in connection with a
2  communications traffic monitoring application to identify randomly occurring traffic
3  patterns.

1    15.    The method of Claim 9, wherein said method is used in connection with a
2  communications network management application to monitor usage of network
3  components.

1    16.    The method of Claim 9, wherein said weighted traffic flow per usage
2  corresponds to the average use of network element per period multiplied by the average
3  communications traffic quantity per use.

1    17.    The method of Claim 9, wherein at least a portion of said communications
2  traffic flows between network elements over the public Internet.

1    18.    A method of predicting expiration of quantity based security associations
2  between network elements, at least a portion of communications traffic exchanged
3  between said network flowing over the public Internet, said method comprising:
4      calculating on a periodic basis a weighted traffic flow per usage for a given
5  network element;
6      comparing a value of said weighted traffic flow per usage with a remainder value
7  of yet to be processed communications traffic of one of said quantity based security
8  associations; and
9      renegotiating another security association with a corresponding one of said
10  network elements if said remainder value is less than said weighted traffic flow.

1    19.    The method of Claim 18, wherein said weighted traffic flow per usage
2  corresponds to the average use of a security association per period multiplied by the
3  average number of bytes processed per use.

1    20.    The method of Claim 18, wherein said security association is an IPSEC
2  security association.